SHARED NETWORK ACCESS USING DIFFERENT ACCESS KEYS

ABSTRACT OF THE DISCLOSURE

[0081]   The invention provides a secure Wi-Fi communications method and system to enable automatic network roaming without requiring any back-end authentication servers and alleviating the need to handle large numbers of network parameters. In an embodiment of the invention, a client device listens for a "beacon frame" broadcast from a Wi-Fi access point. The beacon frame identifies the basic service set identifier (BSSID) of the access point. A tamper-resistant token, or client key, installed at the client device stores a set of authentication parameters, e.g., cryptographic keys, for each Wi-Fi network the client is permitted to access. Each set of authentication parameters is associated with a particular BSSID. Using the BSSID received from the access point, the client device identifies and implements the appropriate set of authentication parameters necessary to authenticate the client device according to an authentication process generally accepted by all the Wi-Fi networks potentially servicing the client. Accordingly, a consistent authentication and security mechanism is provided to enable a client device to easily roam from one network to another without requiring the client to manually change network configurations.